AMENDMENT TO THE CLAIMS

1. (Currently Amended) A computer-implemented method for enhancing the security of communication over a network, the method comprising:

receiving a set of authentication credentials from a user;

receiving from the user a request that requires communication over the network with a remote system;

applying a collection of security privileges to the set of authentication credentials to determine if the user is authorized to carry out the request wherein applying comprises applying based at least in part upon a role-based determination that involves referencing a record that assigns access privileges to various roles that can be assumed by the user;

selectively transmitting a security certificate over the network to the remote system, the certificate containing a public key;

receiving from the remote system a session ticket that has been encrypted with the public key;

decrypting the session ticket with a corresponding private key;

using the session ticket as an authenticator for subsequent communications with the remote system.

2. (Original) The method of claim 1, wherein:

selectively transmitting a security certificate to the remote system comprises selectively transmitting a security certificate to a service provider configured to extend the functionality of a software application by remotely providing a service; and

receiving from the user a request comprises receiving a request for a delivery of said service.

3. (Original) The method of claim 2, wherein selectively transmitting comprises transmitting

only when the collection of security privileges indicates that the user is authorized to receive said service.

4. (Original) The method of claim 3, wherein using the session ticket comprises using the session ticket to secure communications associated with the service provider extending the functionality of a software application.

5. (Original) The method of claim 4, wherein using the session ticket comprises using the session ticket without requiring the user to re-submit the set of authentication credentials.

6. (Original) The method of claim 2, wherein using the session ticket comprises using the session ticket until it expires.

7. (Original) The method of claim 3, wherein:

selectively transmitting a security certificate to the remote system comprises selectively transmitting a security certificate to a remote application configured to extend the functionality of a software application by providing access to information; and

receiving from the user a request comprises receiving a request for access to the information.

8. (Original) The method of claim 1, wherein selectively transmitting a security certificate comprises selectively transmitting a security certificate that contains an embedded indication of the identity of an entity associated with which the user is associated.

9. (Currently Amended) The method of claim 1, wherein applying a collection of security privileges further comprises applying ~~a collection of security privileges wherein~~ access rights that are distributed ~~among~~ relative to a plurality of user accounts. ~~each associated with a different set of authentication credentials.~~

10. (Cancelled)

11. (Currently Amended) The method of claim 9, wherein applying a collection of security privileges comprises applying access rights based at least in part upon a determination of which roles are assigned to a user account associated with a user. ~~a collection of security privileges wherein the plurality of user accounts correspond to a plurality of user roles to which access rights are distributed, wherein multiple users can be assigned to a single user account.~~

12. (Currently Amended) A computer-implemented method for enhancing the security of communication over a network, the method comprising:

generating a public key and a corresponding private key;

storing the private key;

transmitting the public key over the network to a registration service;

receiving from the registration service a security certificate that includes the public key;

transmitting the security certificate over the network to an entity with which a channel of communication is desired;

receiving from the entity a session ticket encrypted with the public key;

decrypting the session ticket with the private key; and

using the session ticket as an authenticator for subsequent communications with the entity, wherein using the session ticket comprises using the session ticket as a cryptography key for encrypting or decrypting messages.

13. (Cancelled)

14. (Original) The method of claim 12, wherein transmitting the security certificate over the network comprises transmitting the security certificate to a service provider configured to extend the functionality of a software application by remotely providing a service.

15. (Original) The method of claim 14, wherein using the session ticket comprises using the session ticket to secure communications with the service provider.

16. (Original) The method of claim 12, wherein transmitting the security certificate over the network comprises transmitting the certificate to a remote peer.

17. (Original) The method of claim 16, wherein transmitting the security certificate over the network comprises transmitting the security ticket from a first application host to a second application host.

18. (Original) A communication security system for facilitating the enhancement of the security of communications over a network, the system comprising:

a client application configured to respond to a user request for service by retrieving a security certificate that contains a public encryption key, and by obtaining a service identifier that corresponds to the user request;

an authorization service configured to receive the security certificate and the service identifier from the client application, and being further configured to selectively generate a corresponding session ticket that is encrypted with the public key, the client application being further configured to receive and decrypt the corresponding session ticket with a private key that corresponds to the public key; and

a service provider configured to receive a service command with the corresponding session ticket after it has been decrypted, and being further configured to validate information contained in the corresponding session ticket and selectively execute the service command.

19. (Original) The method of claim 18, wherein the authorization service is further configured to

again encrypt the corresponding session ticket but this time with a first key portion of a service key pair.

20. (Original) The method of claim 19, wherein the service provider is further configured to decrypt the session ticket with a second key portion of a service key pair.

21. (Original) A method for enabling secure communication between a service provider and a plurality of socket applications installed on multiple computing devices within a local access network, wherein the service provider is configured to extend the functionality of the socket applications by providing services, the method comprising:

creating an account by registering with a centralized authentication service associated with the service provider, wherein registering includes indicating a desire to activate a service supported by the service provider; and

activating each of the plurality of socket applications, wherein activating comprises:

generating a public key and a corresponding private key;

storing the private key;

transmitting the public key over the network, along with an indication of the account, to the centralized authentication service; and

receiving from the authentication service a security certificate that includes the public key.

22. (Original) The method of claim 21, further comprising activating one or more services.

23. (Original) The method of claim 21, further comprising interacting with at least one socket application to configure a set of user access privileges.

24. (Original) The method of claim 19, further comprising:

transmitting the security certificate over the network to the service provider;

receiving from the service provider a session ticket encrypted with the public key;

decrypting the session ticket with the private key; and

using the session ticket as an authenticator for subsequent communications with the entity.

25. (Original) The method of claim 19, wherein registering further comprises receiving an entity token that represents an entity associated with the application sockets.

26. (Original) A computer-implemented method for enhancing the security of communication over a network between multiple peer application hosts, the method comprising:

receiving a security certificate from a first application host;

generating a session ticket;

encrypting the session ticket with a public key contained in the security certificate;

transmitting the session ticket to the first application host; and

receiving a message from the first application host, the message being at least partially encrypted in accordance with the session key prior to its being encrypted with the public key.

27. (Original) The method of claim 26, further comprising:

generating a response message;

encrypting the response message; and

transmitting the message to the first application host.

28. (Original) The method of claim 26, further comprising authenticating the certificate.

29. (Original) The method of claim 26, wherein authenticating the certificate comprises interacting with an authentication service to validate an expression of the first application host's identity.